

## Calculs avec des entiers

Ordres de grandeur, complexité, vitesses pratiques

## Ordres de grandeur

- Taille d'un entier  $n$  :  $t_n = \lceil \log_2(n) \rceil$  bits  $\rightarrow n = O(\exp(t_n))$ 
  - 128 bits = 39 chiffres, 512 bits = 155 chiffres, 1024 bits = 309 chiffres
- Vitesse des ordinateurs
  - 1 GHz =  $10^9$  secondes
  - Lumière du projecteur à la salle : 3m à 300000 km/s =  $10^{-8}$  s
  - Ce portable fait donc 10 additions le temps que la lumière arrive du projecteur !
- Age de l'univers : 15 milliards \* 365 \* 24 \* 3600  $\approx 5 \cdot 10^{17}$  s
- Nombre d'électrons dans l'univers :  $10^{61} * 10^{11} * 10^{12} \approx 10^{84}$
- Complexité d'un algorithme pour des nombres de 128 bits
  - $t_1 = 128$  opérations,  $t_2 = 16384$  ops,  $t_3 = 2 \cdot 10^6$  ops,  $t_4 = 3 \cdot 10^8$  ops
  - $n = 10^{39}$  opérations  $\rightarrow$  2 millions de fois l'âge de l'univers sur un million de PC à 1GHz

## Calcul sur les entiers

- 32 (ou 64) bits : codent entiers de 0 à  $2^{32}-1$ 
  - addition ( $\approx 1$  cycle)
  - soustraction ( $\approx 1$  cycle)
  - multiplication ( $\approx 1$  cycle)
  - division ( $\approx 10$  cycles)
- Pour 1 GHz  $\approx 1$  milliard d'additions/multiplications à la seconde

## Entiers en précision arbitraire

- EX: C/C++ Gnu Multiprecision Package
  - Liste de mots non signés de 32 bits, plus le signe.
  - Addition/soustraction d'entiers bornés par  $n$  :  $O(t_n = \log(n))$  opérations
  - Multiplication :
    - $O(t_n^2)$  opérations (méthode classique)
    - Karatsuba  $O(t_n^{1.585})$
    - Toom-Cook  $O(t_n^{1.465})$
    - Schönhage & Strassen  $O(t_n \log(t_n) \log \log(t_n))$ .
  - $\rightarrow$  En pratique : classique jusqu'à 32 mots ( $\approx 300$  chiffres), Karatsuba jusqu'à 256 mots, première FFT à partir de 10000 mots.
  - Division : cf. multiplication, + divisions sur 32 bits

## Arithmétique classique

- MAops = million d'opérations arithmétiques / seconde
  - $\rightarrow$  Sur un Pentium IV, 2.4GHz, max  $\approx 2400$  MAops
- Mesures : comptent accès mémoire, copie, affectation, opération, ...
- Sur 32 bits machine (long int) :
 

Addition, Soustraction, Multiplication :	365 MAops
Négation :	915 MAops
APXYIN ( $r += a \times b$ ) :	711 MAops
Division :	81 MAops
- Avec GMP,
 

300 bits	3000 bits
- Addition, Soustraction :	2.2
- Multiplication :	0.64
- Négation :	0.017
- APXYIN :	2.6
- Division :	0.85
- APXYIN :	4.5
- Division :	1.1
- APXYIN :	0.035
- Division :	0.03

## Calculs modulaires

Ordres de grandeur, complexité, vitesses pratiques

### Entiers modulaires

- Notation :  $a \equiv b [m]$ , (a est congru à b modulo m)
- si (a-b) est divisible par m. ex:  $11 \equiv 5 [6]$
- $Z/nZ = \{0, 1, \dots, n-1\}$

#### Opérations modulaires classiques :

- Addition/Soustraction : addition d'entiers + décalage de m
  - $x = a + b$
  - $SI (x > m) \text{ Alors } x = x - m$
- Multiplication : multiplication d'entiers + division d'entiers
  - $x = a \times b$
  - $x = x \ \&\ m$  // Calcul du reste de la division de r par m
- Division : pgcd + division d'entiers quand valide

### Algorithme d'Euclide étendu

- Bézout : a et b premiers,  $\exists (u,v), a u + b v = 1 = \text{pgcd}(a,b)$
- Algorithme d'Euclide pour le pgcd :
- $a = b q_1 + r_1; b = r_1 q_2 + r_2; r_1 = r_2 q_3 + r_3 \dots$
- Algorithme d'Euclide étendu, calcule aussi u et v
  1.  $a + 0 b = a$
  2.  $0 a + 1 b = b$
 → Appliquer le pgcd sur 1. et 2.
- Complexité classique :  $O(t^2)$ , ... FFT en  $O(t \log(t)^2)$
- Application : calcul de la division dans un corps premier :
  - $a \equiv 1 [b]$ , i.e. u est l'inverse de a modulo b !
  - Corollaire :  $Z/pZ$  est un corps pour p premier (tout non nul plus petit que p est inversible, puiseque premier avec p)

### Arithmétique MODULAIRE classique

- MApps = million d'opérations arithmétiques / seconde
  - Sur un Pentium IV, 2.4Ghz, max  $\approx$  2400 MApps
- Mesures : comptent accès mémoire, copie, affectation, opération, ...
- Sur 16 bits machine (long int) :
  - Addition, Soustraction : 300 MApps
  - Multiplication : 68 MApps
  - Négation : 475 MApps
  - AXPYIN ( $r + a = a \times b$ ) : 135 MApps
  - Division (Bézout) : 1.6 MApps
- Avec GMP, 32 bits
  - Addition, Soustraction : 3000 bits
  - Multiplication : 1.5
  - Négation : 0.3
  - AXPYIN : 1.7
  - Négation : 1.4
  - AXPYIN : 3
  - Division : 0.55
  - Division : 0.03
  - Division : 0.01

### Implémentation pour premiers en mots machine

- Stockage entre 0 et p-1
- Utilise la division système pour le calcul de la multiplication
- **AXPY**:  $r = (a \times x + y); r = (r < p ? r : r \% p)$
- Addition, soustraction sont rapides
- Multiplication est lente
- Requis :  $(p^2 - p) <$  mots machine (ex. 2<sup>32</sup> pour des *unsigned int* d'une architecture 32 bits)
  - (p-46337 pour 32 bits, p-3037000493 pour 64 bits)

### Implémentation avec inverse numérique

- Stocke une représentation numérique de l'inverse de p
- **AXPY**:  $r = (a \times x + y); r = \text{floor}(r \times 1/p) \times p$
- Multiplication parfois plus rapide (pas de division, mais floor est assez lent également)
- Requier aussi :  $(p^2 - p) <$  taille des mots
- Variante existe avec fmod (reste flottant), attention aux arrondis.

### Utiliser un générateur

- Le groupe des inversibles est cyclique de cardinalité q-1:
    1. Il existe un générateur, g
    2. Chaque inversible est une puissance de g
 Ex. Mod 7 :  $2^1=2, 2^2=4, 2^3=1$ , et  $3^1=3, 3^2=2, 3^3=6, 3^4=4, 3^5=5, 3^6=1$
  - Un générateur des inversibles est une racine primitive
    - Théorème:
      - Si  $m=2, 4, p^k, 2p^k$ , il y a  $\phi(m)$  racines primitives dans  $Z/mZ$
      - Sinon il n'y a pas de racine primitive
- © Si m est premier,  $Z/mZ$  est un corps et il y a  $\phi(m-1)$  racines primitives (il y a même  $\phi(d)$  éléments d'ordre d,  $\forall d \mid (m-1)$ )

### Comment trouver une racine primitive

- Il faut d'abord pouvoir tester si un nombre est générateur
  - Exhaustif, on calcule toutes les puissances jusqu'à trouver 1
  - L'ordre de la divise  $\phi(m)$ , donc si  $v$  p premier et divisant  $\phi(m)$ 

$$\alpha^{\phi(m)} \neq 1 \pmod{m}$$

Alors  $\alpha$  est une racine primitive.

    - Il faut tout de même factoriser  $m$  pour calculer  $\phi(m)$
    - Factorisation partielle  $\rightarrow$  racine probablement primitive
- Ensuite, il faut tester des candidats
  - Dans 80% des cas, il semble qu'il existe une racine primitive  $\leq 6$
  - Tirages aléatoires : en moyenne  $m-1/\phi(m-1) < K \ln(\ln(m))$  essais
  - Moins de 0.1s sur 333MHz, pour  $m < 2^{64}$

### Petits corps premiers : générateurs 1/2

- Pré calcul de 3 tables
  - Moins de 2s de calcul pour des corps avec moins de  $2^{24}$  éléments
- Correspondance entre  $x$  et  $i$  :  $t_1[x] = i$ , tq  $x = g^i$
- Correspondance entre  $i$  et  $x$  :  $t_2[i] = x$ , tq  $x = g^i$
- Table des «  $\#$ is  $\#m$  » :  $t_3[i] = j$ , tq  $1+g^i = g^j$
- [Conway] : faire les opérations sur les indices !
  - $a \times x : (g^i \times g^j) \% m = g^{(i+j) \pm (m-1)}$
  - 0 et 1 ont des valeurs particulières, par exemple 0 et  $m-1$
- [Imamura], [Hubert], [Douillet]  $\rightarrow$  réduisent la taille des tables

### Petits corps premiers : générateurs 2/2

$a = g^i; x = g^j; y = g^k;$   
 $a \times x + y = g^i \times g^j + g^k = g^{(i+j)+k}$

**AXPY:**  $r = (i+j)-k;$   
 $r = t_3[(i+j)+k];$   
 et tests pour zéro, indices modulo  $m-1$  ...

- Absolument aucune multiplication ni division système
- Chaque opération est une combinaison de tests, additions et accès aux tables.

### Réduction de Montgomery

La division système est remplacée par des décalages et des masques

```

#define MASK 0x00000001
#define HALF_MASK 0x00000000
/* #mim le precomputé to -1/p mod B
with the extended gcd */
    
```

**AXPY:**

- $c = (a \times x + y);$  /\*  $c \text{ mod } B$  \*/
- unigned long  $c0$  ( $c \& \text{MASK}$ ); /\*  $c - c/p \text{ mod } B$  \*/
- $c0 = (c0 * \text{nim}) \& \text{MASK};$  /\*  $c0 = 0 \text{ mod } B$  \*/
- $c += c0 * p;$  /\* high bits of  $c$  \*/
- $c >>= \text{HALF\_BITS};$  /\*  $0 < c < 2p$  \*/
- return ( $c - p * c - pic$ );

- Aucune division, très souvent plus rapide de nos jours !
- Premlers plus petits: Taille( $p^2+p$ \*half\_word\_size) < taille des mots
- ( $p < 40499$  pour 32 bits,  $p = 2654435761$  pour 64 bits)

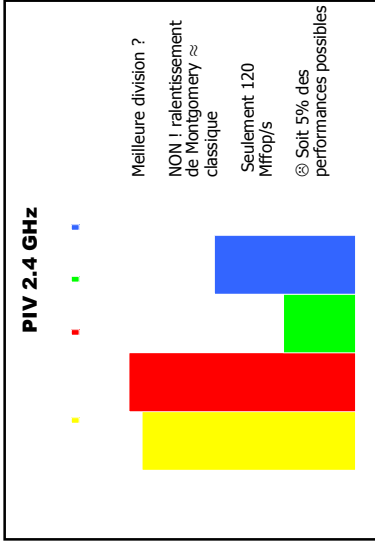
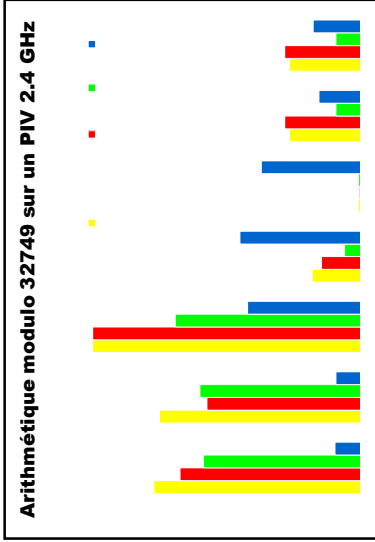
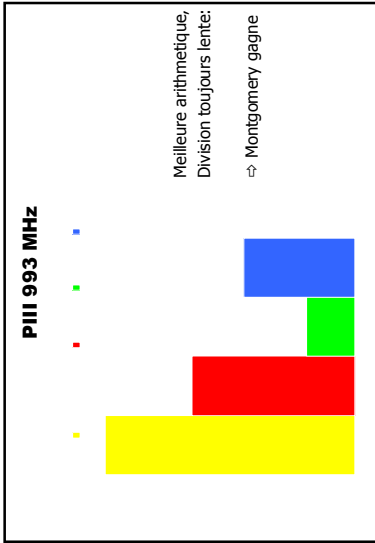
### Sun Ultra 250 MHz

Mémoire rapide / arithmétique machine :

- Faire des Tables
- Tabuler  $p^2$  valeurs est possible au prix de :
  - Tables énormes / défauts de cache
  - additions supplémentaires (Kenane-Muro, MBUS)

### Arithmétique modulo 32749 sur un PIII 993 MHz

Choix d'implémentation dépendant des machines/algo/ithmes



## Corps finis et polynômes

Ordres de grandeur, complexité, vitesses pratiques

### Fondements ensemblistes

- Groupe  $(G, *)$  : \* binaire, interne, associative,  $\exists$  neutre, tout élément possède un inverse.
  - Un groupe est abélien si \* est commutative
  - Un groupe est cyclique si il possède un générateur :
    - $\exists g \in G, \forall a \in G, \exists i \in \mathbb{Z}, a = g^i$
- Anneau  $(A, +, \times)$  :  $(A, +)$  groupe abélien,  $\times$  associative, distributive sur  $+$ ,  $\exists$  neutre pour  $\times$  ( $A$  est unitaire).
  - $A^*$  est l'ensemble des inversibles par  $\times$
  - Ex:  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  et les inversibles sont les premiers avec  $n$
- Corps  $(A, +, \times)$  : anneau et  $A^* = A \setminus \{0\}$ 
  - $\mathbb{R}, \mathbb{C}, \mathbb{Q}$  : infinis
  - Entiers modulo un nombre premier  $p$  ( $\mathbb{Z}/p\mathbb{Z}$ ) : finis de cardinal  $p$

### Anneau des polynômes sur un corps abélien

- $G$  un corps, alors pour  $a_i \in G$ , on écrit  $P = \sum a_i X^i \in G[X]$
- Dans cet anneau, il existe une division euclidienne :
  - $\forall A, B \in G[X] : \exists (Q, R) \in G[X]$  avec  $\deg(R) < \deg(B)$  tels que  $A = BQ + R$
  - Il y a donc un pgcd, et l'Algorithme d'Euclide étendu est valide.
  - Deux polynômes sont premiers entre eux si leur pgcd  $\in G$
  - Un polynôme est irréductible si il est premier avec tous ceux de degré inférieur
- Il y a une factorisation (unique à un facteur de  $G$  près) en polynômes irréductibles.
  - ⊗ Elle est polynomiale ! [Berlekamp], [Cantor-Zassenhaus]
  - Ex: Dans  $\mathbb{Z}/3\mathbb{Z}$ , on a  $X^2+X+1 = (X-1)(X^2+X-1)$

### Complexité des opérations polynomiales

- Addition : d additions du corps
- Multiplication
  - Classique :  $O(d^2)$  additions/multiplications du corps
  - Karatsuba :  $O(d^{1.585})$  additions/multiplications du corps
  - Si corps FFT :  $O(d \log(d))$  additions/multiplications du corps
- Euclide :  $O(\text{Mult}(d) \log(d))$  opérations du corps
- Factorisations
  - [Cantor-Zassenhaus] :  $O(d^2 \log(q))$  opérations de  $\text{GF}(q)$
  - [Berlekamp] :  $O(d^3 + \text{Mult}(d) \log(q))$  opérations de  $\text{GF}(q)$

### Produit rapide de polynômes

$\omega$  racine  $n^{\text{ème}}$  de l'unité

1.  $H = \text{DFT}(P) = [\dots, \sum_j P_j \omega^{j\delta}, \dots]$ 
  - $H_k = P(\omega^k)$
2.  $\text{DFT}(P \cdot Q) = \text{DFT}(P) \cdot \text{DFT}(Q)$  terme à terme
  - $C_k = H_k G_k = P(\omega^k) Q(\omega^k) = PQ(\omega^k)$
3.  $PQ = [\dots, \sum_k C_k \omega^{k\delta}, \dots]$ 
  - $\text{DFT}^{-1}(\text{DFT}(P) \cdot \text{DFT}(Q))$

⇒ Complexité : 3 transformations  $O(n \log(n))$   
 1 produit terme à terme  $O(n)$

### Anneau quotient $\text{GF}[X]/P$

- Pour  $G$  un corps,  $P$  un polynôme de degré  $d$
- l'ensemble des polynômes de degré strictement inférieur à  $d$  et muni de l'addition et de la multiplication modulo  $P$  est un anneau commutatif
- Si  $|G|=q$ , alors  $C$  est un anneau à  $q^d$  éléments
- Si  $P$  irréductible, Euclide nous indique que  $C$  est un corps
- Ex:  $Z/3Z[X] / (X^2+X-1) = \{0, 1, 2, X, X+1, X-1, 2X, 2X+1, 2X-1\}$ 
  - Et  $(X+1)(2X+1) = 2X^2+3X+1 = 2(X^2+X-1)+X = X$
- Proposition :  $\forall p$  premier,  $\forall d > 0$ , Il existe des irréductibles
- Corollaire : Il existe un corps fini de cardinal  $p^d$
- Théorème : ce sont les seuls

### Quelques propriétés des corps finis

- $Q$  et  $Z/pZ$  : corps premiers
- $\text{GF}(q)$  : corps fini ou corps de Galois à  $q$  éléments
- $K = \{k \in \mathbb{N}^*, k, 1_k = 0\}$ ; Caractéristique du corps :
  - 0 si  $K$  est vide (ex:  $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ )
  - Plus petit élément de  $K$  (ex:  $p$  pour  $Z/pZ$ )
  - Caractéristique : 0 ou un nombre premier !
- Cardinal d'un corps fini = puissance de sa caractéristique
- L'ensemble des inversibles d'un corps fini  $\text{GF}(p^k)^*$  est cyclique de cardinal  $p^k-1$
- L'ordre d'un élément est la pp puissance tq  $x^k = 1$ , il divise  $p^k-1$

### Test d'irréductibilité

- Théorème :  $(X^d)^n - X$  est le produit de tous les polynômes unitaires irréductibles de  $\text{GF}(q)[X]$  dont le degré divise  $r$ .
- Test d'irréductibilité [Ben-Or] pour  $P \in \text{GF}(q)[X]$ 
  - Si  $\text{pgcd}(P, P^d) \neq 1$  Alors renvoyer « non »
  - // *Maintenant P est sans carrés*
  - $W = X$
  - Pour  $d=1$  jusqu'à  $d^p / 2$  Faire
    - $W \equiv W^q \pmod{P}$
    - Si  $\text{pgcd}(W-X, P) \neq 1$  Alors renvoyer « non »
  - Renvoyer « oui »

### Construction d'un corps fini

- Combien d'irréductibles de degré  $d$  ?
  - près d'un sur  $d$
- Tirage aléatoire : avec une espérance de  $d$  tirages
- L'arithmétique classique est plus rapide si le polynôme irréductible est creux
  - Ex:  $AB=HX^k+L \pmod{X^d+a}$  =  $-aH + L$
  - Rechercher d'abord des polynômes sous la forme  $X^d+a, X^c+bx^k+a$
- Une fois que l'on a un polynôme irréductible, on a les opérations arithmétiques, le corps est construit !

### Deuxième construction : générateurs

- $GF(q^h)$ \* reste cyclique
  - ⊙ Il existe des générateurs
  - Ex: dans  $Z/3Z[X] / (X^2+X-1) = \{0, 1, 2, X, X+1, X+2, 2X, 2X+1, 2X+2\}$ 
    - $(X+1)^0 = 1$
    - $(X+1)^1 = X+1$
    - $(X+1)^2 = X^2+2X+1 = X+2$
    - $(X+1)^3 = (X+2)(X+1) = 2X$
    - $(X+1)^4 = 2$
    - $(X+1)^5 = 2X+2$
    - $(X+1)^6 = 2X+1$
    - $(X+1)^7 = X$
    - $(X+1)^8 = 1$

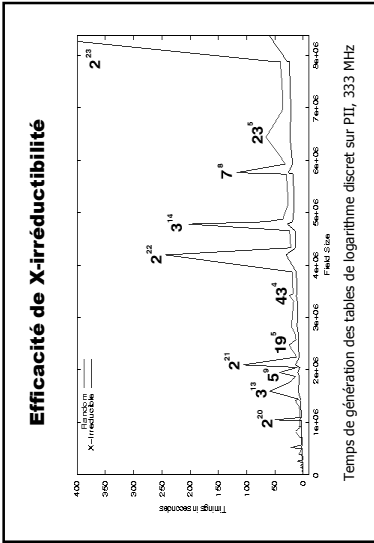
### Tester un générateur

1. Exhaustif, on calcule toutes les puissances de R jusqu'à trouver 1
2. L'ordre de R divise  $q^d-1$ , donc
  - Si  $\forall p$  premier et divisant  $q^d-1$ ,  $R^{(q^d-1)/p} \neq 1 [P]$
  - Alors R est un générateur

- On a remplacé des opérations polynomiales par des opérations sur des indices
- accélération d'un facteur au moins  $d^2$  !

### Polynômes primitifs

- Calcul des tables : calculer toutes les puissances de R
- Plus rapide si P est creux et R est le plus simple possible
- ⊙ Il existe des P tels que X est un générateur
- Appelés primitifs, ou X-irréductibles
- Il y en a  $\phi(q^d-1)/d$  parmi  $p'$  polynômes
- Pour  $p < 2^{32}$ , cela donne une espérance  $< 12d$



### Construction des grands corps finis

- Construction avec tables :
  - ⊙ Arithmétique rapide
  - ⊙ Besoin de  $O(p^2)$  unités de mémoire
  - limitée par la taille de RAM
- Construction polynomiale :
  - ⊙ Pas de problème de mémoire
  - ⊙ Arithmétique polynomiale
- Construction d'un grand corps  $GF(p^2)$  avec  $d=kr$ 
  - Construire  $GF(p^k)$  efficace et tenir en mémoire
  - Trouver un polynôme P irréductible creux de degré r dans  $GF(p^k)$
  - $GF(p^2) \cong GF(p^k)[X]/P$